Junos Pulse für Google Android

Benutzerhandbuch

Release
4.0

Juni 2012
R1

Copyright © 2012, Juniper Networks, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen und ScreenOS sind in den USA und anderen Ländern eingetragene Marken von Juniper Networks, Inc. Das Juniper Networks-Logo, das Junos-Logo und JunosE sind Marken von Juniper Networks, Inc. Alle anderen Marken, Dienstleistungsmarken, eingetragenen Marken oder eingetragenen Dienstleistungsmarken sind Eigentum der jeweiligen Besitzer. Juniper Networks übernimmt keine Haftung für Fehler in diesem Dokument. Juniper Networks behält sich das Recht vor, diese Publikation ohne Ankündigung zu verändern, zu übertragen oder anderweitig zu überarbeiten. Von Juniper Networks hergestellte oder verkaufte Produkte oder Komponenten davon unterliegen möglicherweise einem oder mehreren der folgenden Patente (US-Patentnummern), die sich im Besitz von Juniper Networks befinden oder für Juniper Networks lizenziert sind: Patentnummern 5.473.599, 5.905.725, 5.909.440, 6.192.051, 6.333.650, 6.359.479, 6.406.312, 6.429.706, 6.459.579, 6.493.347, 6.538.518, 6.538.899, 6.552.918, 6.567.902, 6.578.186 und 6.590.785. Copyright © 2012, Juniper Networks, Inc. Alle Rechte vorbehalten.

M8/30/12

Copyright © 2012, Juniper Networks, Inc.

Inhalt

Download und Installation von Junos Pulse 1
Verfügbare Funktionen von Junos Pulse 1
Registrieren von Security 2
Das Mobile Security Dashboard 3
Validierung der E-Mail-Adresse 3
Arbeiten mit den Sicherheitsfunktionen 3
Scan/Bedrohungen wurden entdeckt 3
Sicherung 6
Remote-Überwachung 6
Einstellungen 7
Sicherheitseinstellungen 8
Support-Info 8
Aktualisieren 8
Diebstahlsicherungsfunktionen 9
Kennwortrichtlinien und Speicherverschlüsselung 10
Scream schließen 11
Benutzerdefinierte Schaltfläche 11
Deinstallieren oder Löschen von Daten 11
Hinzufügen einer sicheren Verbindung 12
Herstellen einer Verbindung 12
Symbol "Viewing Connection Status" (Verbindungsstatus anzeigen) 13
Fenster "Viewing Connection Status" (Verbindungsstatus anzeigen) 13
Eingeschränkter Zugriff 13
Benutzeroberflächenmodi 14
Bekannte Probleme und Einschränkungen 14

Installation und Arbeiten mit Junos Pulse für Google Android

Junos Pulse ermöglicht Ihnen den Zugriff auf geschützte Netzwerkressourcen mit Ihrem Google Android™-Gerät. Ihr Gerät wird auch gegen Viren und Malware geschützt und enthält Tools, um die potenziellen Risiken eines verloren gegangenen oder gestohlenen Geräts zu verringern.

Weitere Informationen zu Junos Pulse und zu unterstützten Plattformen finden Sie unter http://www.juniper.net/support/products/pulse/mobile/

Download und Installation von Junos Pulse

Folgen Sie den folgenden Anweisungen, um die Junos Pulse-Software auf Google Android-Geräten zu installieren.

Informativer Hinweis: Der Junos Pulse-Client steht im Google Play-Anwendungs-Store zur Verfügung.

1. Laden Sie von Ihrem Android-Gerät aus die Junos Pulse-Software direkt auf Ihr Gerät. Nach dem Download wird Junos Pulse automatisch installiert.
2. Nach dem Download und der Installation wird das Junos Pulse-Symbol im Anwendungsmenü angezeigt.

3. Wenn Sie Junos Pulse das erste Mal starten, wird die Endbenutzer-Lizenzvereinbarung angezeigt. Sie müssen die Lizenz **akzeptieren**, um Junos Pulse verwenden zu können.

Verfügbare Funktionen von Junos Pulse

Informativer Hinweis: Junos Pulse kann mit allen verfügbaren Funktionen oder mit Unterfunktionen, die auf den Anforderungen des Benutzers basieren, bereitgestellt werden. Möglicherweise stehen Ihnen auf Ihrem Gerät nicht alle hier beschriebenen Junos Pulse-Funktionen zur Verfügung.

Junos Pulse kann folgende Funktionen enthalten:

Registerkarte "Sicherheit"

- **Scan/Bedrohungen wurden entdeckt**: Führt auf dem Gerät gefundene Bedrohungen auf, und gibt Ihnen die Möglichkeit, verdächtige Anwendungen zu erlauben oder zu entfernen. Wenn keine Bedrohungen gefunden wurden, steht auf dieser Schaltfläche "Scan". Wenn Bedrohungen gefunden wurden, steht auf dieser Schaltfläche "Bedrohungen wurden entdeckt".
- **Sicherung**: Erlaubt Ihnen, Ihre Kontakte und Kalendereereignisse zu sichern.
- **Remote-Überwachung**: Stellt Informationen dazu bereit, welche Geräteaktivitäten überwacht werden.
- **Diebstahlsicherung**: Führt die Diebstahlsicherungsfunktionen auf, die auf Ihrem Gerät aktiviert sind.
- **Benutzerdefinierte Schaltfläche**: Stellt einen Link zu einer angepassten URL bereit, über den Sie zu einer durch Ihren Dienstanbieter bereitgestellten Webseite gelangen.

Registerkarte "VPN"

Informativer Hinweis: Dieser Dienst wird nur angeboten, wenn Sie über eine sichere Verbindung auf Ressourcen des Firmennetzwerks zugreifen.

Copyright © 2012, Juniper Networks, Inc.

- **Verbindungen**: Ermöglicht Ihnen das Hinzufügen, Bearbeiten und Entfernen von Netzwerkverbindungen des Unternehmens.
- **Intranet**: Gibt die vom Administrator bereitgestellten Weblinks an.
- **E-Mail**: Startet die E-Mail-Anwendung.
- **Status:** Mit dieser Funktion können Sie bei auftretenden Problemen die Protokolldateien anzeigen, löschen und per E-Mail versenden. Die Protokolldateien enthalten Einträge zu allen Sicherheitsbelangen wie Virenscanzeiten und entdeckte Viren. Wenn Sie eine VPN-Verbindung eingerichtet haben, können Sie den Status dieser Verbindung von diesem Fenster aus anzeigen.

Registrieren von Security

Die Junos Pulse Mobile Security-Suite stellt einen Zugriff auf Funktionen bereit, die Ihr Gerät vor Malware und Viren schützen und Ihnen erlauben, die Kalender- und Kontaktinformationen des Geräts auf einem zentralen Server zu sichern. Sie müssen Ihr Gerät registrieren, bevor Sie auf die Sicherheitsfunktionen zugreifen können.

Sie können Ihr Gerät über eine automatische URL-Registrierung oder einen manuellen Registrierungsprozess registrieren.

Automatische URL-Registrierung

Für die automatische URL-Registrierung muss eine vom Administrator oder vom Dienstanbieter bereitgestellte URL ausgewählt werden. Wenn Sie die URL auswählen, werden Sie aufgefordert zu bestätigen, dass die URL von einer vertrauenswürdigen Quelle stammt. Wenn Sie in dieser Aufforderung auf **Ja** tippen, findet der automatische Sicherheitsregistrierungsprozess statt.

Gehen Sie folgendermaßen vor, um Sicherheitsfunktionen automatisch zu registrieren:

1. Starten Sie Junos Pulse.
2. Wählen Sie die Registrierungs-URL aus, die Ihnen über eine E-Mail, eine Textnachricht oder eine Webseite bereitgestellt wurde.
3. Da durch die automatische Registrierung die Sicherheitseinstellungen auf Ihrem Gerät geändert werden, sollten Sie die Gültigkeit der URL überprüfen. Wenn Sie sicher sind, dass die URL vertrauenswürdig ist, wählen Sie **Ja** aus, wenn Sie dazu aufgefordert werden.

Wenn Sie "Ja" ausgewählt haben, wird Ihr Gerät automatisch für Sicherheitsfunktionen registriert.

Manuelle Registrierung

In manchen Fällen müssen Sie bei der manuellen Registrierung eine URL auswählen. Wenn Sie die URL ausgewählt haben, werden Sie aufgefordert zu bestätigen, dass die URL von einer vertrauenswürdigen Quelle stammt. Wenn Sie in der Registrierungsaufforderung auf "Ja" tippen, wird das Fenster für die manuelle Registrierung angezeigt.

Im Registrierungsfenster müssen Sie Informationen wie den durch den Administrator oder den Dienstanbieter bereitgestellten Lizenzcode eingeben.

Informativer Hinweis: Wenn Sie ein reines WIFI-Gerät verwenden (z. B. ein Tablet ohne Mobilfunknetz), wird das Telefonnummernfeld nicht im Registrierungsfenster angezeigt.

Gehen Sie folgendermaßen vor, um Sicherheitsfunktionen manuell zu registrieren:

1. Starten Sie Junos Pulse.
2. Wählen Sie die **URL** aus, die Ihnen über eine E-Mail, eine Textnachricht oder eine Webseite bereitgestellt wurde.
3. Überprüfen Sie, dass die URL vertrauenswürdig ist, und tippen Sie auf **Ja**, wenn Sie dazu aufgefordert werden. Das Registrierungsfenster wird angezeigt.
4. Geben Sie eine **E-Mail-Adresse** und ein **Kennwort** ein.
5. Geben Sie den **Lizenzcode** an.

Copyright © 2012, Juniper Networks, Inc.

6. Die Telefonnummer Ihres Geräts steht im Feld **Telefonnummer**. Wenn die Nummer nicht angezeigt wird, geben Sie sie manuell mit Ländercode und Ortskennzahl ohne internationale Vorwahlen ein: '00' oder '+'. Verwenden Sie keine Leerzeichen, Klammern oder Sonderzeichen. Überprüfen Sie, dass Telefonnummern zwischen 11 und 15 Ziffern lang sind (einschließlich Ländercode).
7. Wählen Sie **Register**.

Das Mobile Security Dashboard

Das Dashboard ist einer der Server, mit denen Sie Ihr Gerät registrieren. Wenn Sie Zugriff auf das Dashboard erlangen (dieser Zugriff kann für Sie optional von einem Administrator oder einem Dienstanbieter eingerichtet werden), können Sie sich anmelden, um Ihr Gerät zu überwachen, einige Sicherheitseinstellungen zu steuern und Ihre E-Mail-Adresse und Ihr Kennwort zu ändern. Sie können auf die Dashboard-Web-Schnittstelle über eine bereitgestellte URL aus zugreifen. Informationen zur Dashboard-Anmeldung und zur Konfiguration finden Sie in der Junos Pulse Mobile Security Dashboard-Dokumentation.

Validierung der E-Mail-Adresse

Nach Ihrer ersten Anmeldung am Dashboard erhalten Sie eine E-Mail, in der Sie aufgefordert werden, Ihre E-Mail-Adresse zu validieren. In dieser E-Mail ist ein Link enthalten, auf den Sie klicken müssen, um Ihre E-Mail-Adresse zu validieren. Nachdem Sie auf den Link geklickt haben, wird eine Webseitenbenachrichtigung angezeigt, um Sie zu informieren, dass Ihre E-Mail-Adresse validiert wurde.

Arbeiten mit den Sicherheitsfunktionen

Nach Ihrer erfolgreichen Registrierung wird die Bestätigung **Activate device administrator** (Geräteadministrator aktivieren) angezeigt, wenn auf Ihrem Gerät Android 2.2 oder höher ausgeführt wird.

Informativer Hinweis: Wenn Sie den Geräteadministrator nicht aktivieren, verhalten sich manche Funktionen anders. In den folgenden Abschnitten finden Sie weitere Informationen: “Diebstahlsicherungsfunktionen” auf Seite 9 und “Deinstallieren oder Löschen von Daten” auf Seite 11.

Wenn Sicherheitsfunktionen registriert werden, werden die verfügbaren Funktionen angezeigt. Über die Registerkarte "Sicherheit" können Sie jetzt darauf zugreifen. Folgende Funktionen stehen zur Verfügung:

- **Scan/Bedrohungen wurden entdeckt**: Führt auf dem Gerät gefundene Bedrohungen (Viren und Malware) auf und gibt Ihnen die Möglichkeit, verdächtige Anwendungen zu erlauben oder zu entfernen. Wurden keine Bedrohungen gefunden, steht auf dieser Schaltfläche "Scan". Tippen Sie darauf, um zum Scanfenster zu gelangen. Wurden Bedrohungen gefunden, steht auf dieser Schaltfläche "Bedrohungen wurden entdeckt". Tippen Sie darauf, um die entdeckten Bedrohungen anzuzeigen.

- **Sicherung**: Erlaubt Ihnen, Ihre Kontakte und Kalendereereignisse zu sichern.
- **Remote-Überwachung**: Stellt Informationen dazu bereit, welche Geräteaktivitäten überwacht werden.
- **Einstellungen**: Über die Menütaste verfügbar. Über die Einstellungen können Sie Scanintervalle einrichten, Supportinformationen und Anwendungsprotokolle anzeigen, sowie Virussignaturen und die Junos Pulse-Software aktualisieren.

Scan/Bedrohungen wurden entdeckt

Die Anti-Virus und Malwareentdeckung schützt Ihr Gerät, indem alle Dateien und SD-Karten gescannt werden, um einen Befall zu verhindern. So zeigen Sie Bedrohungen an und konfigurieren Einstellungen für die Entdeckung von Bedrohungen:

Copyright © 2012, Juniper Networks, Inc.

1. Starten Sie Junos Pulse.
2. Gehen Sie zur Registerkarte **Sicherheit**.
3. Wenn Bedrohungen gefunden wurden, tippen Sie auf die Schaltfläche **Bedrohungen wurden entdeckt**. Sie gelangen zum Fenster "Scanergebnisse".
4. Im Fenster "Scanergebnisse" werden die Viren, Malware, verdächtige Anwendungen und in die Blacklist eingetragene Anwendungen, die auf dem Gerät gefunden wurden, aufgeführt. Wenn auf Ihrem Gerät nicht die Erkennung von Bedrohungen aktiviert ist, sehen Sie nur die in die Blacklist eingetragenen Anwendungen, die auf dem Gerät gefunden wurden.

Informativer Hinweis: In der Leiste "Notification" (Benachrichtigung) wird folgende Benachrichtigung angezeigt, wenn eine Bedrohung entdeckt wird.

Registerkarte "Funde"

Jedes erkannte Element wird in der Registerkarte "Funde" angezeigt. Sie können die orange Schaltfläche neben dem entdeckten Element auswählen, um weitere Informationen zur Erkennung anzuzeigen und die verfügbaren Aktionen zu sehen. Folgende Erkennungsarten und zur Verfügung stehenden Aktionen sind vorhanden:

- **In Blacklist eingetragene Anwendung**: Dies ist eine Anwendung, die in die Blacklist eingetragen wurde. Zum Entfernen einer in die Blacklist eingetragenen Anwendung wählen Sie die **orange Schaltfläche** neben dem Anwendungsnamen, und tippen Sie auf die zur Verfügung stehende Schaltfläche **Deinstall**. Wenn Sie Anwendungen, die in der Blacklist eingetragen wurden, nicht deinstallieren, wird das Benachrichtigungssymbol weiterhin oben im Junos Pulse-Fenster angezeigt.

Informativer Hinweis: Bei manchen Geräten kann Junos Pulse Anwendungen, die in der Blacklist eingetragen wurden, automatisch deinstallieren.

- **Kritische Malware**: Dies ist eine auf Ihrem Gerät installierte Anwendung, von der bekannt ist, dass sie Malware ist. Zum Entfernen von Malware wählen Sie die **orange Schaltfläche** neben dem Anwendungsnamen, und tippen Sie auf die zur Verfügung stehende Schaltfläche **Deinstall**. Wenn Sie als Malware erkannte Anwendungen nicht deinstallieren, wird das Benachrichtigungssymbol weiterhin oben im Junos Pulse-Fenster angezeigt.

Informativer Hinweis: Bei manchen Geräten kann Junos Pulse Anwendungen, die als Malware erkannt wurden, automatisch deinstallieren.

Copyright © 2012, Juniper Networks, Inc.

- **Verdächtige Anwendung**: Dies ist eine auf Ihrem Gerät installierte Anwendung, die verdächtig erscheint. Die verdächtige Bezeichnung wird auf eine Anwendung angewendet, wenn durch Heuristiken bestimmt wird, dass es sich bei der Anwendung ggf. um Malware handelt. Bei verdächtigen Anwendungen haben Sie die Option, die Anwendung zu erlauben (zur weißen Liste hinzuzufügen) oder sie zu deinstallieren. Zum Zulassen einer verdächtigen Anwendung wählen Sie die **orange Schaltfläche** neben dem Anwendungsnamen, und tippen Sie auf die zur Verfügung stehende Schaltfläche **Allow** (Zulassen). Sie müssen auch auf **Ja** tippen, um das Zulassen zu bestätigen. Tippen Sie anschließend auf **OK**, um zu bestätigen, dass Ihnen klar ist, dass diese Aktion ein potenzielles Risiko für das Gerät bedeutet. (Sie können das letzte Dialogfeld ausblenden, sodass es nicht mehr angezeigt wird.)

  Zum Deinstallieren einer verdächtigen Anwendung wählen Sie die **orange Schaltfläche** neben der Anwendung, und tippen Sie auf die Schaltfläche **Deinstall**. Wenn Sie verdächtige Anwendungen weder deinstallieren noch zulassen, wird das Benachrichtigungssymbol weiterhin oben im Junos Pulse-Fenster angezeigt.

  Tippen Sie auf die Schaltfläche **Details anzeigen**, um auf weitere Informationen zu den verdächtigen Anwendungen zuzugreifen. Sie können die Anwendung auch vom Detailfenster aus zulassen oder deinstallieren.

- **Virus**: Während des letzten Scans gefundene Viren werden in der Registerkarte "Funde" aufgeführt. Es wird empfohlen, hier angezeigte Viren zu löschen. Zum Löschen des Virus vom Gerät tippen Sie auf die **orange Schaltfläche** neben dem Virusnamen, und tippen Sie auf die Schaltfläche **Entfernen**. Tippen Sie auf die Schaltfläche **Details anzeigen**, um auf weitere Informationen zum erkannten Virus zuzugreifen. Sie können den Virus auch vom Detailfenster aus entfernen.

- **Schaltfläche Scannen**: Die Schaltfläche **Scannen** oben in der Registerkarte **Funde** zeigt an, wann das zuletzt verwendete Gerät gescannt wurde. Sie können auf die Schaltfläche **Scannen** tippen, um ein Fenster zu öffnen, von wo aus Sie eine der drei Gerätescanarten starten können. Wählen Sie eine der folgenden Scanoptionen, und tippen Sie auf **OK**, um den Scanvorgang zu starten.

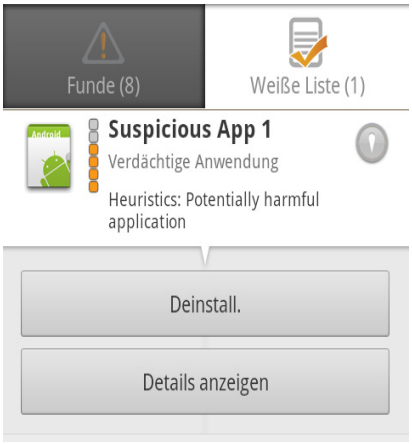
  - **Anwendungsscan**: Scannt alle Nicht-Systemanwendungen.
  - **Anwendungs- und SD-Kartenscan**: Scannt alle Nicht-Systemanwendungen und die SD-Karte.
  - **Vollständiger Gerätescan**: Scannt alle Dateien, Nicht-Systemanwendungen und die SD-Karte.

Informativer Hinweis: Wenn Sie einen vollständigen Gerätescan manuell starten, wird ggf. eine Akkunutzungswarnung angezeigt. Dies dient zur Information, dass Scans ggf. die Akkulaufzeit stark verringern. Deshalb sollten Sie das Gerät während des Scannens aufladen.

Copyright © 2012, Juniper Networks, Inc.

Registerkarte "Weiße Liste"

- Wenn Sie eine erkannte verdächtige Anwendung zulassen, wird sie in der Registerkarte "Weiße Liste" angezeigt. Von der Registerkarte "Weiße Liste" aus können Sie verdächtige Anwendungen verwalten, falls Sie Ihre Meinung ändern und eine zugelassene Anwendung zu einem späteren Zeitpunkt deinstallieren möchten. Wenn Sie auf die **orange Schaltfläche** neben dem Anwendungsnamen und auf die zur Verfügung stehende Schaltfläche **Deinstall.** tippen, können Sie die Anwendung in der weißen Liste deinstallieren. Für weitere Informationen können Sie auch auf die Schaltfläche **Details anzeigen** tippen, um weitere Informationen zur Anwendung anzuzeigen und die Anwendung anschließend vom Detailfenster aus zu deinstallieren.



Sicherung

Junos Pulse Mobile Security sichert Kontakt- und Kalenderinformationen an einem zentralen Speicherort. Zur Wiederherstellung von Daten müssen Sie Ihren Administrator kontaktieren oder auf das Dashboard zugreifen. Eine Wiederherstellung erfolgt über einen SMS-Befehl, über den Ihr Gerät den Server kontaktieren soll, um Ihre Sicherung abzurufen.

So sichern Sie Gerätedaten:

1. Starten Sie Junos Pulse.
2. Gehen Sie zur **Registerkarte Sicherheit**.
3. Wählen Sie **Sicherung**. Der Zeitpunkt der letzten Sicherung wird auf der Schaltfläche "Sicherung" angezeigt.
4. Im Sicherungsfenster werden die zuvor gesicherten Kontakte und Kalenderereignisse angezeigt. Tippen Sie zum Starten einer Sicherung oben im Fenster auf die Schaltfläche **Sicherung**. Die Sicherung beginnt sofort.

Remote-Überwachung

Über das Fenster "Remote-Überw." können Sie die überwachten Ereignistypen und die Aktivitäten des Geräts anzeigen. Gehen Sie zum Anzeigen des Fensters "Remote-Überw." folgendermaßen vor:

1. Starten Sie Junos Pulse.
2. Gehen Sie zur Registerkarte **Sicherheit**.
3. Wählen Sie **Remote-Überw**.

Copyright © 2012, Juniper Networks, Inc.

Das Fenster "Remote-Überw." zeigt eine oder mehrere der folgenden überwachten Aktivitäten an:

Überwachung

- SMS: Ein- und ausgehende SMS-Nachrichten werden mit Absender, Empfänger und Inhalt jeder Nachricht protokolliert.
- MMS: Die Protokollierung von MMS-Nachrichten wird derzeit nicht unterstützt.
- Voice (Sprachanrufe): Die Anrufliste wird protokolliert, z. B. gestartete ausgehende Anrufe und empfangene eingehende Anrufe (die Gesprächsdauer wird nicht aufgezeichnet, doch die Remote-Telefonnummer wird aufgezeichnet.)
- Log images/pictures (Bilder protokollieren): Wenn dies auf dem Server aktiviert wurde, werden heruntergeladene oder mit dem Gerät aufgenommene Bilder in Miniaturbilder umgewandelt und auf den Server hochgeladen. Dies geschieht sofort und unabhängig von Protokolleinschränkungen.

Protokolle:

- Event limit (Grenzwert Ereignis): Wenn die Gesamtanzahl an Ereignissen (SMS, E-Mail, Sprachanrufe) diesen Grenzwert überschreitet, werden alle Protokolle auf den Server hochgeladen.
- File size limit (Grenzwert Dateigröße): Wenn die gesamte Dateigröße aller Protokolle (SMS, E-Mail, Sprachanrufe) diesen Grenzwert überschreitet, werden alle Protokolle auf den Server hochgeladen. Beachten Sie, dass SMS-Nachrichten i. d. R. mehrere hundert Bytes groß sind. E-Mails liegen normalerweise im Bereich von 2 KB oder größer (ohne Anhänge). Sprachnachrichten liegen i. d. R. im Bereich von 200 Bytes.

Steuerung:

- Periodic GPS updates (GPS-Aktualisierungszeitraum): Dieser Aktualisierungszeitraum wird auf dem Server konfiguriert. Über diese Einstellung wird die Geräteposition regelmäßig abgefragt und zur Nachverfolgung auf den Server hochgeladen.
- Block calls (Anrufe sperren): Bei Aktivierung werden alle ausgehenden Anrufe gesperrt.

Einstellungen

Vom Fenster "Einstellungen" aus können Sie Sicherheitseinstellungen wie Scanoptionen und Aktualisierungsintervalle der Virusunterschrift konfigurieren. Sie können auch Supportinformationen und Protokolldateien anzeigen.

In der Junos Pulse-Anwendung können Sie über die Schaltfläche **Einstellungen** auf das Fenster "Einstellungen" zugreifen. Gehen Sie folgendermaßen vor, um die Schaltfläche "Einstellungen" aufzufinden:

- Tippen Sie auf die drei vertikalen Punkte rechts auf der **Aktionsleiste** (bei Android 4.0 und höher), um auf das Menü zuzugreifen. Wählen Sie aus dem Menü **Einstellungen** aus.

- Tippen Sie auf die Schaltfläche **Menü** (Android 3.0 und älter), um auf das Menü zuzugreifen. Wählen Sie aus dem Menü **Einstellungen** aus.

Copyright © 2012, Juniper Networks, Inc.

Vom Fenster "Einstellungen" aus können Sie auf Folgendes zugreifen:

Sicherheitseinstellungen

Die Sicherheitseinstellungen werden vom Administrator oder Dienstanbieter konfiguriert, und Änderungen werden auf Ihr Gerät geladen. Sie können Sicherheitseinstellungen ändern, indem Sie auf den **orangen Pfeil** neben den **Sicherheitseinstellungen** tippen, um auf Folgendes zuzugreifen:

- **Anwendungen bei der Installation scannen**: Wenn diese Option aktiviert ist, wird ein Scanvorgang gestartet, wenn eine Anwendung installiert wird. Ein Scan für Malware findet auch bei Dateien statt, die nach /sdcard/download heruntergeladen werden. Wenn diese Option deaktiviert ist, wird nur zum geplanten Zeitpunkt oder bei einem manuellen Start gescannt. Aktivieren Sie das Kontrollkästchen, um diese Funktion zu aktivieren.
- **SD-Karte beim Einlegen scannen**: Scannt die SD-Karte auf Malware und Viren. Aktivieren Sie das Kontrollkästchen, um diese Funktion zu aktivieren.
- **In Archiven scannen**: Der Inhalt komprimierter Dateien, wie z. B. ZIP- und APK-Dateien, wird gescannt.
- **Medien-Scanning optimieren**: Ermöglicht, dass Foto-, Medien- und Musikdateien schneller gescannt werden, indem schon gescannte Dateien nicht noch einmal gescannt werden (außer diese Dateien haben sich geändert).
- **Vollständiger Gerätescan**: Zeigt die Zeitintervalle an, zu denen ein vollständiger Gerätescan stattfindet. Bei einem vollständigen Gerätescan werden alle Dateien, die SD-Karte und Nicht-Systemanwendungen gescannt. Tippen Sie auf den Pfeil neben dem Zeitintervall, um das Scanintervall zu ändern.
- **Profilaktualisierung**: Virusdefinitionen werden bei der Registrierung geladen und nach einem voreingestellten Zeitplan aktualisiert. Tippen Sie auf den Pfeil neben dem Zeitintervall, um das Aktualisierungsintervall zu ändern.

Support-Info

Sie können Informationen zum Gerät und der Junos Pulse-Anwendung anzeigen, sowie Protokolle anzeigen und senden, indem Sie auf den **orangen Pfeil** neben **Support-Info** im Fenster **Einstellungen** tippen. Sie gelangen zum Fenster "Support-Info", wo Sie Folgendes machen können:

- Tippen Sie auf die Schaltfläche **Protokolle anzeigen**, um die Protokolldateidaten anzuzeigen. In diesem Datenfenster können Sie aus der Pulldownliste auswählen, welche Protokollart angezeigt werden soll. Sie haben außerdem die Möglichkeit, die Protokolldatei zu löschen, indem Sie auf die Schaltfläche **Protokolle löschen** tippen.
- Tippen Sie auf die Schaltfläche **Protokolle senden**, um eine Anwendung auszuwählen, von der aus Sie die Protokolldatei senden möchten.

Informativer Hinweis: Protokolldateien können nur über eine E-Mail-Anwendung gesendet werden. Derzeit werden keine anderen Methoden unterstützt.

Aktualisieren

Sie können die Virenliste und die Junos Pulse-Anwendung aktualisieren (falls für beide Aktualisierungen vorhanden sind), indem Sie auf den **orangen Pfeil** neben **Update (Aktualisieren)** im Fenster **Einstellungen** tippen. Sie gelangen zum Fenster "Update" (Aktualisieren). Hier können Sie für folgende Elemente nach Aktualisierungen suchen:

- **Virus List (Virenliste)**: Wenn eine Aktualisierung verfügbar ist, tippen Sie auf die Schaltfläche **Update (Aktualisieren)**, um Ihre Virenliste zu aktualisieren. Wenn die Schaltfläche "Update" (Aktualisieren) nicht vorhanden ist, ist Ihre Liste wahrscheinlich aktuell. Über die Schaltfläche **Prüfen** können Sie nach Aktualisierungen suchen.

Copyright © 2012, Juniper Networks, Inc.

- **Anwendung**: Wenn für Junos Pulse eine Aktualisierung verfügbar ist, tippen Sie auf die Schaltfläche **Update (Aktualisieren)**, um Ihre Software zu aktualisieren. Wenn die Schaltfläche "Update" (Aktualisieren) nicht vorhanden ist, ist Ihre Software wahrscheinlich aktuell. Über die Schaltfläche **Prüfen** können Sie nach Aktualisierungen suchen.

Diebstahlsicherungsfunktionen

Es gibt eine Reihe von Maßnahmen, die Sie ergreifen können, wenn Ihr Gerät verloren gegangen ist oder gestohlen wurde. Wenn diese Funktionen in der Junos Pulse-Bereitstellung sichtbar sind, wird auf der Startseite von Junos Pulse die Schaltfläche **Diebstahlsicherung** angezeigt. Wenn Sie auf diese Schaltfläche tippen, werden die auf Ihrem Gerät aktivierten Diebstahlsicherungsfunktionen aufgeführt.

Sie können im Fenster **Diebstahlsicherung** auf die Schaltfläche Diebstahlsicherungsfunktionen verwalten tippen, um zur Webseite Ihres Dienstanbieters zu gelangen, von wo aus Sie weitere Diebstahlsicherungsfunktionen ansehen oder kaufen können.

Beispiele für Diebstahlsicherungsfunktionen:

- **Lock Handset** (Handset sperren) und **Unlock Handset** (Handset entsperren): Das Gerät wird gesperrt, bis vom Server ein Befehl zum Entsperren an das Gerät gesendet wird oder ein Gerätekennwort eingegeben wird, das der Gerätekennwortrichtlinie entspricht. Wenn vom Server ein Sperrbefehl an das Gerät gesendet wird, kann auch ein neues Kennwort erstellt werden. Dieses Kennwort kann per E-Mail an Sie gesendet werden, und Sie können es ändern. Wenn mit diesem neu erzeugten Kennwort der Sperrbefehl ausgelöst wird, kann Folgendes auf verschiedenen Geräten passieren:
  - Wenn der Geräteadministrator aktiviert ist und für das Gerät schon ein Kennwort konfiguriert wurde:
    - Wenn ein Sperrbefehl mit einem neuen Kennwort gesendet wurde, wird das Gerät mit dem bestehenden Kennwort gesperrt. Das neue Kennwort vom Server wird nicht verwendet.
    - Wenn ein Sperrbefehl mit einem leeren Kennwort gesendet wird, wird das Gerät mit dem bestehenden Kennwort gesperrt. Das Kennwort vom Server wird nicht verwendet.
  - Wenn der Geräteadministrator aktiviert ist und für das Gerät noch kein Kennwort konfiguriert wurde:
    - Wenn ein Sperrbefehl mit einem neuen Kennwort gesendet wurde, wird das Gerät mit diesem neuen Kennwort gesperrt.
    - Wenn ein Sperrbefehl mit einem leeren Kennwort gesendet wird, wird das Gerät NICHT gesperrt.
  - Wenn der Geräteadministrator deaktiviert ist und das Gerät automatisch registriert wird:
    - Wenn ein Sperrbefehl mit einem neuen Kennwort gesendet wurde, wird das Gerät mit diesem neuen Kennwort gesperrt. (Unabhängig vom auf dem Gerät konfigurierten Kennwort.)
    - Wenn ein Sperrbefehl mit einem leeren Kennwort gesendet wird, wird das Gerät NICHT gesperrt.

Copyright © 2012, Juniper Networks, Inc.

- Wenn der Geräteadministrator deaktiviert ist und das Gerät manuell registriert wird:
  - Wenn ein Sperrbefehl mit einem neuen Kennwort gesendet wurde, wird das Gerät mit diesem neuen Kennwort gesperrt. (Unabhängig vom auf dem Gerät konfigurierten Kennwort.)
  - Wenn ein Sperrbefehl mit einem leeren Kennwort gesendet wird, wird das Gerät NICHT gesperrt.

- **Schaltfläche Notru**f: Wenn das Gerät gesperrt ist, steht die Schaltfläche "Notruf" über das Entsperrfenster zur Verfügung. Sie können einen Notruf tätigen, wenn Sie auf diese Schaltfläche tippen und eine Notrufnummer eingeben, zum Beispiel 112.
- **SIM-Änderung**: (Bei Android 2.2 und höher) Wenn die Geräteadministratorfunktion und "Vollständige Löschung" aktiviert sind, wird das Gerät durch einen Löschbefehl auf die Werkseinstellungen zurückgesetzt. Eine Sperre wird nicht ausgeführt. Wenn die Geräteadministratorfunktion nicht aktiviert ist und die SIM-Karte ausgewechselt wird, wechselt das Gerät in den GPS-Diebstahlmodus, und das Gerät wird gesperrt.
- **SIM-Änderung**: (Bei Android 2.1) Das Gerät wechselt in den GPS-Diebstahlmodus, und das Gerät wird gesperrt. Wenn "Vollständige Löschung" aktiviert ist, werden vertrauliche Geräteinformationen automatisch gelöscht.
- **Wipe Handset (Handset löschen)**: (Bei Android 2.2 und höher) Wenn die Geräteadministratorfunktion aktiviert ist, wird das Gerät durch einen Löschbefehl auf die Werkseinstellungen zurückgesetzt. Wenn die Geräteadministratorfunktion nicht aktiviert ist, werden durch einen Löschbefehl Planungs-, Kontakt- und Aufgabeninformationen, SMS-Nachrichten und die Speicherkarte gelöscht.
- **Wipe Handset (Handset löschen)**: (Bei Android 2.1) Löscht Planungs-, Kontakt- und Aufgabeninformationen.
- **Send Backup (Sicherung senden)**: Wenn diese Daten nicht auf dem Server gespeichert werden, werden über diese Funktion die Sicherungsinformationen vom Gerät gesammelt und per E-Mail an die während der Registrierung angegebene E-Mail-Adresse an Sie gesendet.
- **GPS Location (GPS-Standort)**: Wenn Ihr Gerät mit GPS ausgestattet ist, kann der Administrator das Gerät auffinden. Der Gerätestandort wird auf dem Junos Pulse-Server angezeigt.
- **Alarm On and Off (Scream locate) (Alarm An und Aus (Scream-Ortung)**: Es ertönt ein Alarmton in höchster Lautstärke, um das Gerät an einem Ort in der Nähe aufzufinden.
- **GPS Theft On and Off (GPS-Diebstahl An und Aus)**: Sendet im Zeitraum von 2 bis 5 Minuten GPS-Aktualisierungen an den Junos Pulse-Server, um den GPS-Standort abzugleichen, wenn das Gerät gestohlen wurde.

Kennwortrichtlinien und Speicherverschlüsselung

Junos Pulse kann Kennwort- und Speicherverschlüsselungsrichtlinien auf Ihrem Gerät erzwingen. Dies bedeutet, dass Sie ein Gerätekennwort verwenden und eine Datenverschlüsselung für das Gerät einrichten müssen, welche den Kriterien der Junos Pulse-Sicherheitsrichtlinie entsprechen.

In einer Kennwortrichtlinie können Anforderungen enthalten sein, sind jedoch nicht darauf beschränkt, wie z. B. die Anzahl der benötigten Zeichen, wie oft Kennwörter geändert werden müssen, die Anzahl der fehlerhaften Kennworteingaben, bevor das Gerät gelöscht wird und wie lange das Gerät sich im Ruhezustand befinden kann, bevor es automatisch gesperrt wird. Sie können das Kennwort auch aus der Ferne zurücksetzen und an Sie per E-Mail senden lassen. Wenn Ihr Gerät z. B. aus der Ferne gesperrt wurde, kann ein Entsperrbefehl Ihr Kennwort mit dem neuen Kennwort zurücksetzen, das an Sie in einer E-Mail gesendet wurde.

Copyright © 2012, Juniper Networks, Inc.

Wenn Sie kein Gerätekennwort eingerichtet haben oder Ihr Kennwort nicht die Anforderungen der Kennwortrichtlinien erfüllt, werden Sie aufgefordert, Ihr Kennwort zurückzusetzen, sodass es den Anforderungen entspricht.

Als Teil der Sicherheitsrichtlinie des Geräts müssen Sie ggf. Ihre Anwendungsdaten verschlüsseln. Wenn dies der Fall ist, werden Sie über ein Aufforderungsfenster über diese Anforderung informiert. Sie werden fortlaufend aufgefordert, bis Sie auf Ihrem Gerät die Datenverschlüsselungsfunktion einrichten. Wenn Sie die Anforderungen der Sicherheitsrichtlinien nicht in einem bestimmten Zeitraum erfüllen, ist es möglich, dass das Gerät aus der Ferne gesperrt oder gelöscht wird.

Scream schließen

Vom Dashboard aus kann an das Gerät ein Scream-Befehl gesendet werden, über den Sie das Gerät akustisch orten können, wenn es sich in Hörweite befindet, selbst wenn die Laufsprecher und der Rufton stumm geschaltet sind. Wenn Sie das Gerät aufgefunden haben, können Sie Scream über die Leiste **Notification** (Benachrichtigung) ausschalten. Wählen Sie die Benachrichtigung **Scream activated** (Scream aktiviert), um den Scream zu schließen.

Benutzerdefinierte Schaltfläche

Wenn diese Funktion in der Junos Pulse-Bereitstellung sichtbar ist, wird eine weitere Schaltfläche auf der Startseite angezeigt, die von Ihrem Dienstanbieter angepasst wurde. Wenn Sie auf diese Schaltfläche tippen, gelangen Sie über eine angepasste URL zu einer von Ihrem Dienstanbieter eingerichteten Webseite. Auf dieser Seite wird Ihnen ggf. angeboten, weitere Funktionen zu kaufen, oder zusätzliche Informationen werden bereitgestellt. Dies unterscheidet sich je nach Dienstanbieter.

Deinstallieren oder Löschen von Daten

Sie müssen ggf. Ihr Gerät nach der Erstregistrierung erneut registrieren, oder Sie müssen die Junos Pulse-Einstellungen aus einem anderen Grund löschen. Sie können dies ausführen, indem Sie Junos Pulse deinstallieren oder indem Sie alle Einstellungen wie folgt manuell löschen.

1. Tippen Sie im Hauptmenü auf **Einstellungen** > **Anwendungen** > **Manage Applications (Anwendungen verwalten)** > **Junos Pulse**.
2. Tippen Sie auf die Schaltfläche **Deinstall.**, um Junos Pulse zu deinstallieren,

oder

3. tippen Sie auf die Schaltfläche **Clear data (Daten löschen)**, um alle Junos Pulse-Daten zu löschen.

Wenn die Funktion **Device Administrator (Geräteadministrator)** aktiviert ist, können Sie Junos Pulse folgendermaßen deinstallieren:

1. Tippen Sie auf der Startseite auf **Einstellungen**> **Location & Security (Standort & Sicherheit)** (auf manchen Geräte nur **Security (Sicherheit)**).
2. Tippen Sie auf **Device Administrator (Geräteadministrator)**, und deaktivieren Sie das Kontrollkästchen **Junos Pulse**. Jetzt können Sie mit der normalen Deinstallation beginnen.

Copyright © 2012, Juniper Networks, Inc.

Hinzufügen einer sicheren Verbindung

Informativer Hinweis: Dieser Dienst wird nur angeboten, wenn Sie über eine sichere Verbindung auf Ressourcen des Firmennetzwerks zugreifen.

Junos Pulse nutzt die 3G-, 4G-, Edge- oder WiFi-Verbindungsfunktion Ihres Geräts, um eine authentifizierte Verbindung mit einem geschützten Netzwerk herzustellen. Sie können für jedes benötigte Netzwerk eine Verbindung hinzufügen. Dies ist eine sichere VPN-Verbindung zu einem Unternehmensnetzwerk oder einem Core-Zugriff-SSL-Kanal zu vom Administrator konfigurierten Weblesezeichen.

Gehen Sie folgendermaßen vor, um eine Verbindung zu definieren:

1. Starten Sie Junos Pulse.
2. Tippen Sie in der Registerkarte **VPN** auf **Verbindungen**.
3. Tippen Sie auf **Verbindung hinzufügen**.
4. Geben Sie die Verbindungseigenschaften wie folgt ein:
   - **Verbindungsname**: Ein beschreibender Name.
   - **URL**: Die vom Webadministrator angegebene Webadresse.

   (Beachten Sie, dass der Verbindungsname und die URL beim Erstellen eines Verbindungsprofils die einzigen erforderlichen Felder sind. Alle weiteren Felder sind optional.)
   - **Benutzername**: Geben Sie Ihren Benutzernamen ein.
   - **Bereich**: Wenn der Administrator diese Informationen bereitgestellt hat, geben Sie den Bereichswert ein.
   - **Rolle**: Wenn der Administrator diese Informationen bereitgestellt hat, geben Sie den Rollenwert ein.
   - **Verwendet Zertifikat**: Aktivieren Sie dieses Kontrollkästchen, wenn der Administrator Ihnen ein digitales Zertifikat bereitgestellt hat. Wenn Sie kein Zertifikat verwenden, müssen Sie beim Anmelden ggf. einen Benutzernamen und ein Kennwort eingeben.
   - **Zertifikatspfad**: Dieses Feld ist verfügbar, wenn Sie das Kontrollkästchen "Verwendet Zertifikat" aktivieren. Wählen Sie **Pick**, um zur Zertifikatdatei zu navigieren. (Beachten Sie, dass dieses Feld erforderlich ist, wenn Sie "Verwendet Zertifikat" ausgewählt haben.)
   - **Schlüsselpfad**: Dieses Feld ist verfügbar, wenn Sie das Kontrollkästchen "Verwendet Zertifikat" aktivieren. Wählen Sie **Pick**, um zu dem vom Administrator bereitgestellten Netzwerkschlüssel zu navigieren. (Beachten Sie, dass dieses Feld erforderlich ist, wenn Sie "Verwendet Zertifikat" ausgewählt haben.)
5. Wählen Sie **Verbindung erstellen**. Ihre Verbindung ist jetzt hergestellt und gespeichert.

Herstellen einer Verbindung

Wenn Sie Ihre Verbindung konfiguriert haben, tippen Sie auf die Schaltfläche **Verbinden**.

Wenn im Feld **Verbindung auswählen** nicht standardmäßig die richtige Verbindung angezeigt wird, können Sie sie aus dem Pulldownmenü auswählen. Gegebenenfalls müssen Sie weitere Informationen, die vom Netzwerk bei der Herstellung einer Verbindung benötigt werden, eingeben.

Copyright © 2012, Juniper Networks, Inc.

Symbol "Viewing Connection Status" (Verbindungsstatus anzeigen)

Der Status Ihrer aktuellen Verbindung wird auch unten im Junos Pulse-Fenster als Symbol angezeigt. Die Darstellung des Symbols zeigt an, ob die Verbindung aktiv, inaktiv oder durch Nichteinhaltung von Richtlinien eingeschränkt ist (siehe Eingeschränkter Zugriff auf Seite 13).

Aktive Verbindung Keine Sitzung Eingeschränkter Zugriff

Das Symbol für eine aktive Verbindung wird auch in der Statusleiste oben in Ihrem Gerätefenster angezeigt. Wenn Sie Junos Pulse schließen, ist dieses Symbol sichtbar, solange Ihre VPN-Verbindung aktiv ist.

Fenster "Viewing Connection Status" (Verbindungsstatus anzeigen)

Wenn Sie eine hergestellte, vollständige VPN-Verbindung haben (nicht alle Geräte unterstützen die vollständigen VPN-Funktionen), können Sie folgende VPN-Informationen anzeigen, wenn Sie auf die Schaltfläche **Status** im Hauptfenster tippen:

- VPN-Status: Verbunden oder Verbindung getrennt
- Server: Server-URL
- Dauer
- Gesendete Bytes
- Empfangene Bytes
- Adresse

Von der Leiste "Notification" (Benachrichtigung) aus wird bei einer aktiven VPN-Verbindung auch folgende Benachrichtigung angezeigt.

Informativer Hinweis: Wenn Sie nur Zugriff auf Weblesezeichen (Core-Zugriff anstatt VPN-Zugriff) haben, ist der VPN-Status "Disconnected" (Verbindung getrennt), aber das Junos Pulse-Verbindungssymbol wird unten im Junos Pulse-Fenster angezeigt.

Eingeschränkter Zugriff

Zur Sicherstellung der Integrität der Mobilgeräte, die auf Netzwerkressourcen zugreifen, kann ein Administrator eine Sicherheitsrichtlinie erzwingen, die Mobilgeräte für eine Netzwerkverbindung erfüllen müssen. Wenn entdeckt wird, dass ein Gerät beim Versuch einer sicheren Netzwerkverbindung nicht den Richtlinien entspricht, wird ggf. nur ein eingeschränkter Netzwerkzugriff gewährt. Wenn Ihr Gerät nicht den Richtlinien entspricht, werden Ihnen die diesbezüglichen Informationen und ggf. die Schaltfläche **Weiter** angezeigt. Tippen Sie auf diese Schaltfläche, um eingeschränkten Netzwerkzugriff zu erhalten.

Beispiele für Gründe, warum Richtlinien nicht eingehalten werden:

- Ihr Gerät hat einen Stamm.
- Auf Ihrem Gerät wird ein Betriebssystem ausgeführt, das nicht durch die Sicherheitsrichtlinie zugelassen ist.
- Ihr Gerät ist nicht aktiv bei dem entsprechenden Mobile Security Gateway (MSG) registriert, und/oder die Junos Pulse Mobile Security-Suite ist auf Ihrem Gerät nicht aktiv.

Sie müssen das Problem der Nichteinhaltung der Richtlinie auf Ihrem Gerät beheben, bevor Sie eine vollständige Netzwerkverbindung herstellen können.

Copyright © 2012, Juniper Networks, Inc.

Benutzeroberflächenmodi

Der Administrator oder der Dienstanbieter kann Junos Pulse auf Ihrem Gerät mit unterschiedlichen Funktionen bereitstellen, die Ihnen über die Junos Pulse-Benutzeroberfläche zur Verfügung stehen. Sie können eine vollständige Benutzeroberfläche haben, bei der alle möglichen Junos Pulse-Funktionen sichtbar sind, oder Sie können eine Mindest- oder Sicherheits-Benutzeroberfläche haben, bei der Junos Pulse-Unterfunktionen von für Sie sichtbaren Funktionen enthalten sind. Folgende mögliche Benutzeroberflächenmodi kann Ihr Administrator auf Ihrem Gerät bereitstellen:

- **Vollständige UI**: In der vollständigen Benutzeroberfläche sind alle verfügbaren Junos Pulse-Funktionen enthalten, wie sie in diesem Handbuch beschrieben werden.
- **Minimal-UI**: In der minimalen Benutzeroberfläche sind der Junos Pulse-Begrüßungsbildschirm und die EULA enthalten. Auf einer Startseite wird das Menü "Info zu" bereitgestellt. Nur bei unterstützten Geräten werden erkannte Viren, Malware und in die Blacklist eingetragene Anwendungen automatisch gelöscht. Bei Malware und bei in der Blacklist eingetragenen Anwendungen wird eine Benachrichtigung angezeigt, wenn eine Anwendung entfernt wird. Wenn Sie auf eine Benachrichtigung tippen, wird eine Seite mit Informationen zur entfernten Anwendung angezeigt. Sie können auf die Schaltfläche **Löschen** tippen, um die Benachrichtigung zu entfernen.
- **Sicherheits-UI**: In der Sicherheits-Benutzeroberfläche sind nur die Junos Pulse-Sicherheitsfunktionen enthalten. Die Möglichkeit, VPN-Verbindungen herzustellen, wird nicht bereitgestellt.

Bekannte Probleme und Einschränkungen

- Android hat bei der Unterstützung von Zertifikaten Einschränkungen. Wenn der Fehler "No cert" (Kein Zertifikat) auftritt oder wenn Junos Pulse beim Verbindungsversuch unerwartet schließt, wenden Sie sich an Ihren Administrator.
- Zu diesem Zeitpunkt können Sie Protokolldateien nur per E-Mail senden. Andere Methoden werden nicht unterstützt.
- Obwohl die Foto- und Videofreigabe als Option angezeigt wird, wenn Sie "Protokolle senden" auswählen, ist dies keine gültige Methode für das Senden von Protokollen. Sie sollten diese Option beim Senden von Protokolldateien nicht auswählen.
- Wenn das Gerät entweder über den Befehl "Handset-Sperre" oder den Befehl "Sperren bei SIM-Änderung" gesperrt wird, können Sie ggf. weiterhin auf die Startseite und das Fenster "Benachrichtigungen" zugreifen.
- Wenn ein Gerät keinen Mobildienst hat, kann es keine Befehle empfangen. Wenn ein Gerät z. B. nur über WiFi verbunden ist, werden Befehle wie Sperren und Löschen nicht vom Gerät empfangen.
- Wenn der Geräteadministrator nicht aktiviert ist, sind die Funktionen zur automatischen Entfernung von Malware, von in der Blacklist enthaltenen Anwendungen, sowie von Anwendungen nur auf bestimmten Samsung-Geräten verfügbar. Weitere Informationen finden Sie im Junos Pulse Supported Platforms Guide (Handbuch für unterstützte Plattformen von Junos Pulse).
- Wenn Ihr Gerät sich mithilfe der automatischen Registrierung bei dem MSG registriert und "Sperren bei SIM-Änderung" aktiviert ist und Sie die SIM-Karte wechseln, kann das Gerät nur entsperrt werden, indem die ursprüngliche SIM-Karte wieder in das Gerät eingelegt wird oder indem ein Entsperrbefehl vom Dashboard an das Gerät gesendet wird.

Copyright © 2012, Juniper Networks, Inc.

Index

A

aktualisieren 8
Anwendung herunterladen 1
automatische Anwendungsentfernung 4
automatische URL-Registrierung 2

B

Bedrohungen wurden entdeckt 3
benutzerdefinierte Schaltfläche 11
Benutzeroberflächenmodi 14

D

Dashboard 3
Daten löschen 11
Daten sichern 6
deinstallieren 11
Diebstahlsicherungsfunktionen 9
- Alarm an und aus, Scream-Ortung 10
- GPS-Diebstahl 10
- GPS-Standort 10
- Handset entsperren, neuen Zugangscode einrichten 9
- Handset sperren, neuen Zugangscode einrichten 9
- Schaltfläche "Notruf" 10
- Sicherung senden 10
- SIM-Änderung 10

E

eingeschränkter Zugriff, Nichteinhaltung 13
Einstellungen 7
E-Mail-Adresse validieren 3
E-Mail-Adressvalidierung 3
EULA 1

G

Geräteadministrator 3

I

in Archiven scannen 8
in Blacklist eingetragene Anwendungen 4
Installation 1

K

Kennwortrichtlinie 10

L

Lizenzcode 2

M

Malware-Anwendungen 4
manuelle Registrierung 2
Medien-Scanning optimieren 8
Mobile Security Dashboard 3

P

Profilaktualisierung 8
Protokolle anzeigen 8
Protokolle senden 8

R

Registerkarte "Funde" 4
Reine WIFI-Geräte 2
Remote-Überwachung 6

S

Scanergebnisse
- in Blacklist eingetragen 4
- in Blacklist eingetragene Anwendungen 4
- Malware 4
- verdächtig 5
- Viren 5

Schaltfläche "Notruf" 10
Schaltfläche "Scannen" 5
Scream schließen 11
Sichere Verbindung 12
Sicherheitseinstellungen 8
Sicherheitsfunktionen 2
- automatische URL-Registrierung 2
- manuelle Registrierung 2
- Registrierung 2
- Virenschutz, Malwareentdeckung 3

Speicherverschlüsselung 10
Support-Info 8

V

Verbinden 12
- Benutzername 12
- Bereich 12
- Hinzufügen einer Verbindung 12
- Rolle 12
- Schlüssel 12
- Statusseite, vollständiges VPN 13
- Statussymbol 13
- URL 12
- Zertifikat 12

Copyright © 2012, Juniper Networks, Inc.

verdächtige Anwendungen 5
verfügbare Funktionen 1
Viren 5
Virenschutz 3

Copyright © 2012, Juniper Networks, Inc.